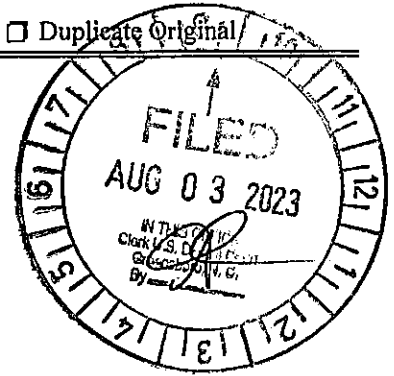


☒ Original☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the
Middle District of North Carolina

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)
 INFORMATION ASSOCIATED WITH ONE IP
 ADDRESS THAT IS STORED AT PREMISES
 CONTROLLED BY HEG US, INC.

Case No. 1:22MJ28-1

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Missouri
 (identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 02/08/2022 (not to exceed 14 days)☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Joe L. Webster
 (United States Magistrate Judge)

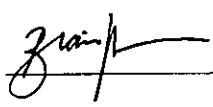
☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____Date and time issued: 1/25/2022 9:40 am

Judge's signature

City and state: Durham, North Carolina

Joe L. Webster, U.S. Magistrate Judge
 Printed name and title

Return		
Case No.: 1:22MJ <u>28</u>	Date and time warrant executed: <u>01/25/2022 3:30 PM</u>	Copy of warrant and inventory left with: <u>HEG US, Inc.</u>
Inventory made in the presence of: <u>N/A</u>		
Inventory of the property taken and name(s) of any person(s) seized: • Letter • CD • Hard drive		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p>		
Date: <u>07/20/2023</u>	 Executing officer's signature	
	<u>Blair Newman, Special Agent</u> Printed name and title	

ATTACHMENT A
PROPERTY TO BE SEARCHED

This warrant applies to information associated with the following Internet Protocol address that are stored at premises owned, maintained, controlled, or operated by HEG US, Inc. ("HEG"), a web hosting company headquartered at 210 North Tucker Boulevard in St. Louis, Missouri:

207.38.84.195

ATTACHMENT B
PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by HEG US, INC. ("Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of Provider, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Provider is required to disclose the following information to the government for each server assigned the Internet Protocol ("IP") address listed in Attachment A:

- a. all records or other information pertaining to each IP address, including all files, databases, and database records stored by Provider in relation to that IP address or identifier;
- b. a forensic image or snapshot of all data and information electronically stored on the servers or droplets, including memory and deleted files, that host each IP address;
- c. all information in the possession of Provider that might identify the subscribers related to that IP address, including names, addresses, telephone numbers and other identifiers, email addresses, business information, the length of service (including start date), means and source of

payment for services (including any credit card or bank account number), and information about any domain name registration;

d. all records pertaining to the types of service utilized by the user; and

e. all records pertaining to communications between Provider and any person regarding the IP address, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within fourteen days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I, for each IP address listed in Attachment A, that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 1030(a)(5)(A) (computer fraud) and 371 (conspiracy to commit computer fraud) in the form of the following:

1. Records and information revealing, referencing, or constituting the operation of the Emotet malware and botnet;

2. Records and information revealing or referencing persons who either collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation, or communicated with

the account about matters relating to the criminal activity under investigation, including records that help reveal their location;

3. Records and information revealing and referencing how and when the account was accessed or used as part of the operation of the Emotet malware and botnet;

4. Transactional and location information pertaining to any items authorized to be seized under this section (Section II);

5. All bank records, checks, credit card bills, account information, and other financial records used to carry out the criminal activity under investigation;

6. Files, databases, and database records stored by Provider referencing, revealing, or constituting the operation of the Emotet malware and botnet;

7. Subscriber information related to the account(s) established to host the IP address in Attachment A, to include:

- a. Names, physical addresses, telephone numbers and other identifiers, email addresses, and business information; and
- b. Length of service (including start date), types of service utilized, means and source of payment for services (including any credit card or bank account number), and billing and payment information.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, a complete copy of the disclosed electronic data may be delivered to the custody and control of attorneys for the government and their support staff for their independent review.